UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/473,522	12/28/1999	KENNETH A. PARULSKI	78744PRC	1080

1333 7590 07/12/2005

BETH READ
PATENT LEGAL STAFF
EASTMAN KODAK COMPANY
343 STATE STREET
ROCHESTER, NY 14650-2201

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/473,522	PARULSKI ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 remain for examination. The correspondence filed 5/9/05 added claims 22-25.

Response to Arguments

2. Applicant's arguments filed 5/9/05 have been fully considered but they are not persuasive.

Applicant argues, "*The applicants respectfully disagree with these observations, in particular finding no such teaching or suggestion in Silverbrook that a processor located within a digital camera generates a random seed.*" Applicant is directed to Silverbrook, col. 173, line 35 through col. 175, line 2, wherein a processor within the camera that generates a random number is rather clearly disclosed.

Applicant further argues, "*As the Examiner noted, Silverbrook in column 151 says that 'random number generators are also often used to generate keys' but then Silverbrook goes on to say (lines 12-13) that 'it is therefore best to say at the moment, that all generators are insecure for this purpose'.*" Examiner respectfully submits that Applicant's citation is taken out of context, in view of the fact that Silverbrook subsequently outlines circumstances in which deterministic random number generators are acceptable (lines 25-35), including the BBS algorithm implemented in a processor as disclosed above. Referring back to col. 173 of Silverbrook, Applicant has helpfully noted that the Silverbrook disclosure teaches wherein "the **seed for R** [emphasis Examiner's] must NOT be generated with a computer-run random number generator."

(lines 50-51). From the text it is readily apparent that the "seed for R" is a value that is separate and distinct from the randomly-generated number R, which in turn is used as a seed for various computations requiring the use of a random number; such random numbers generated by this process are of sufficiently acceptable randomness that they can be (and indeed, are) used within the camera disclosed by Silverbrook (lines 55-60). Thus, the various passages from the Silverbrook disclosure that Applicant has cited are not intended to be a blanket condemnation against all uses of a deterministic random number generator within the processor of a digital camera; rather, these passages are merely cautionary statements advising one of ordinary skill in the art that when using such a generator, it is vitally important that the initial seed for the generator be created non-deterministically, and ideally should be truly random (e.g. col. 174, lines 46-47).

Alternatively, assuming arguendo that the random number R generated by this processor was unfit for [its disclosed] use, Silverbrook also teaches a method by which a random seed can be generated non-deterministically by the Authentication Chip by means of hashing data from a random test image (col. 204, lines 10-20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the random data generated in this manner for all disclosed uses of random values, for precisely all the reasons that Applicant has stressed in the previous correspondence.

With respect to Applicant's traversal of the rejections of claims 2-5, Examiner maintains that any alleged deficiencies in the teachings of Glass are remedied by the teachings found in Silverbrook, as detailed above. Thus, the rejection of these claims in view of the combination of Safai, Silverbrook, and Glass remains proper.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 22-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Silverbrook (U.S. Patent 6,788,336).

Regarding claim 22:

Silverbrook discloses improvements to a digital camera comprising:

(a) a processor located within the digital camera for generating the private key, at least in part, from a physically random process (col. 173, line 35 – col. 175, line 2; col. 193, line 35 – col. 195, line 35; and col. 204, lines 10-20), and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the digital image to produce the image authentication signature (Figs. 182-186).

Regarding claim 23:

Silverbrook discloses all the limitations of claim 22 above. Silverbrook further discloses including an image sensor for capturing images, and wherein the physically

random process is dependent upon a random seed produced from a random noise level in a captured image (col. 204, lines 10-20).

Regarding claim 24:

Silverbrook discloses all the limitations of claim 23 above. Examiner takes Official Notice that the random images taken by the image sensor in the Silverbrook disclosure would necessarily contain random dark fields [relative to other portions of the image that are lighter in color], and that this data would necessarily be incorporated into the random number generated by the disclosed process (Ibid).

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1, 6-21, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Safai et al. (U.S. Patent 6,167,469) and Silverbrook (U.S. Patent 6,788,336).

Referring to Claim 1:

Safai discloses a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising: (a) a processor located within

the digital camera for generating private key and a public key (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29); and (b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed and for using the random seed to generate a private key and a public key."

Silverbrook discloses a processor located within a digital camera that generates a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and teaches using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required public and private keys. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 6:

Safai discloses a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera, the improvement comprising the steps of:

(a) generating a private key in the digital camera (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29); and

(b) storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 7:

Safai discloses a method of authenticating an image captured by a digital camera, comprising the steps of:

(a) generating a private key and a public key in the digital camera (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29);

(b) storing the private key in a memory in the digital camera (col. 16, lines 1-10, 20-35);

(c) communicating the public key to a user (col. 4, lines 5-15);

(d) capturing a digital image (col. 5, lines 35-45; col. 15, lines 60-65);

(e) hashing the captured digital image in the digital camera to produce an image hash (col. 16, lines 1-10);

(f) encrypting the image hash in the digital camera with the private key to produce a digital signature (col. 16, lines 20-35); and

(g) authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 16, lines 10-20).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13, col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required public key and private key. The motivation for doing so would be to potentially increase the

security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 8:

Safai discloses a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of:

(a) manufacturing a digital camera with an internal processor for generating a public key and private key, storing the private key in a memory in the digital camera and communicating the public key to a camera operator;

(b) sending the digital camera to an authentication service;

(c) activating the digital camera at the authentication service to produce the public key and private key, and registering the public key at the authentication service; and

(d) sending the digital camera to a user.

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the

digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 9:

Safai discloses a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values, the improvement comprising:

(a) a processor located within the digital camera for generating a public key and a private key (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29); and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature and the metadata signature (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the

digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 10:

Safai discloses a method of producing an image authentication signature in a digital camera, comprising the steps of:

(a) capturing a digital image (col. 15, lines 60-65);

(b) compressing the captured digital image (col. 14, lines 15-25);

(c) generating, a public key and private key in the digital camera (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29);

(d) storing the private key in a memory in the digital camera (col. 16, lines 1-10, 20-35);

(e) providing one or more metadata values (col. 16, lines 1-15);

(f) hashing the compressed captured digital image and at least one of the metadata values to produce an image hash (col. 16, lines 1-10); and

(g) encrypting the image hash to produce the image authentication signature (col. 16, lines 20-30).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55; col. 173, line 35 – col. 175, line 2) and using a random seed to generate keys (col. 151, lines 12-13; col. 193, line 25 – col. 195, line 25).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, lines 15-20).

Referring to Claim 11:

Safai in view of Silverbrook discloses the limitations of Claim 10 above. Safai further discloses storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values (col. 12, lines 1-15; col. 14, lines 10-25; col. 16, lines 1-10).

Referring to Claim 12:

Safai in view of Silverbrook discloses the limitations of Claim 10 above. Safai further discloses the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature (col. 16, lines 1-40).

Referring to Claim 13:

Safai in view of Silverbrook discloses the limitations of Claim 10 above. Safai further discloses wherein the encrypting step includes encrypting the image hash with the private key to produce the image authentication signature (col. 16, lines 25-40); and further including the step of authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 16, lines 10-25).

Referring to Claim 14:

Safai in view of Silverbrook discloses the limitations of Claim 1 above. Safai further hashing the uncompressed captured digital image to produce a random number k (col. 16, lines 1-10); and wherein the encrypting step includes using the random number k to produce the image authentication signature (col. 16, lines 20-35).

Referring to Claim 15:

Safai in view of Silverbrook discloses the limitations of Claim 1 above. Safai further discloses the encrypting step further produces a metadata signature corresponding to the one or more metadata values (col. 16, lines 1-10; col. 12, lines 50-60).

Regarding claims 16-21:

Safai in view of Silverbrook discloses the limitations of Claims 1 and 6-10 above. Safai also discloses firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory (col. 7, lines 50-55).

Neither Safai nor Silverbrook explicitly disclose "wherein the algorithm is deleted from the firmware memory after the private key is generated." However, Silverbrook teaches that an attacker could gain control of the program [algorithm] used to generate a random seed and use it to reverse engineer a private key, while not being authorized to do so (col. 155, line 55-60). This suggests that it would be desirable to delete the algorithm used to generate a private key after the unique private key for a digital camera has been generated. Furthermore, Silverbrook also teaches that another method of defeating the protection afforded by the authentication chip is to reverse engineer the chip so as to determine the inner workings of the algorithms contained therein (col. 156, lines 55-60). In addition, as noted previously by Applicant, Silverbrook discloses that the keys should only be produced at the place of manufacture, implying that the consumers/end-users has no valid reason to possess any means to create or alter keys themselves (e.g. col. 200, lines 30-45). All of these facts suggest that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Safai and Silverbrook to delete the algorithm from the firmware memory after the private key is generated, in order to prevent it from falling into the wrong hands.

Regarding claim 25:

Silverbrook teaches or suggests all the limitations of claim 24 above. Silverbrook does not appear to disclose a variable gain amplifier, although it does disclose an analog-to-digital conversion mechanism (col. 9, lines 20-25). However, Safai discloses

(i) a variable gain amplifier coupled to the image sensor (col. 5, lines 45-60);

(ii) an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images (col. 5, lines 50-60); and

(iii) the processor causing the variable gain amplifier to be in a high gain condition when the initial test image is captured (col. 5, lines 55-60).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the above into the digital camera disclosed by Silverbrook. The motivation for doing so would be to facilitate the ability to improve or modify image quality (Safai, col. 5, lines 60-62).

7. Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Safai and Silverbrook as applied to claim 1 above, and further in view of Glass et al. (U.S. Patent 6,332,193).

Referring to Claim 2:

Safai in view of Silverbrook discloses the limitations of Claim 1 above. Safai further discloses an image sensor for capturing images (col. 5, lines 30-40).

Safai does not explicitly disclose "the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the captured image is used in producing the random seed". It should be noted that Silverbrook apparently does suggest this (col. 173, line 35 – col. 175, line 2; col. 193, line 25 – col. 195, line 25; col. 204, lines 10-20).

In any case, Glass discloses that the processor includes means for producing a random seed for the private key processing an image captured from the image sensor so that the random noise level in the captured image is used in producing [the random seed, by hashing an initial test image captured by the digital camera] (col. 4, lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Safai and Silverbrook such that the random seed used to generate the private key is generated based on sensor information, as suggested by Glass. One of ordinary skill in the art would have been motivated to do this because it would provide a private key that is easily changed and random.

Referring to Claim 3:

The combination of Safai, Silverbrook, and Glass discloses the limitations of Claim 2 above. Safai further discloses

(i) a variable gain amplifier coupled to the image sensor (col. 5, lines 45-60);

(ii) an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images (col. 5, lines 50-60); and

(iii) the processor causing the variable gain amplifier to be in a high gain condition when the initial test image is captured (col. 5, lines 55-60).

Referring to Claim 4:

Safai in view of Silverbrook discloses the limitations of Claim 1 above.

Safai does not explicitly disclose "the processor includes one or more algorithms for producing a random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing." It should be noted that Silverbrook apparently does suggest this (col. 173, line 35 – col. 175, line 2; col. 193, line 25 – col. 195, line 25; col. 204, lines 10-20).

In any case, Glass discloses wherein the processor includes one or more algorithms for producing the random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing (col. 3, line 60-col. 4, line 15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Safai in view of Silverbrook such that authentication is applied to an image using a random number. One of ordinary skill in the art would

have been motivated to do this because it would allow the user to authenticate the image (col. 3, lines 60-65).

Referring to Claim 5:

The combination of Safai, Silverbrook, and Glass discloses the limitations of Claim 4 above. Safai further discloses the processor includes an image processing algorithm which uses JPEG compression (col. 14, lines 15-25).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- U.S. Patent 5,732,138 issued to Noll et al. "Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system"
- Schneier, Bruce. "Applied Cryptography (Second Edition)". ©1996 Bruce Schneier. Published by John Wiley and Sons Inc. pages 173-174 and 258-261.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
7/6/05

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100